為ESA/SMA SAML SSO生成和配置自簽名證書

目錄

簡介

本文檔介紹如何為安全宣告標籤語言(SAML)服務提供商(SP)配置建立自簽名證書。

必要條件

使用此文檔為郵件安全裝置(ESA)和安全管理裝置(SMA)上的安全宣告標籤語言(SAML)2.0單一登入(SSO)服務提供商(SP)配置生成自簽名證書。

需求

方法1(ESA Web UI):Web UI中的ESA管理訪問許可權和管理證書的許可權。

方法2（OpenSSL指令）：OpenSSL已安裝，可從命令列獲得。

Windows:安裝OpenSSL。

macOS、Linux或Unix:OpenSSL通常在預設情況下或通過作業系統包管理器提供。

採用元件

沒有具體的硬體和軟體要求。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文適用於使用安全宣告標籤語言(SAML)2.0單一登入(SSO)的電子郵件安全裝置(ESA)和安全管理裝置(SMA)部署。SAML SP配置需要安全套接字層(SSL)證書用於服務提供商設定。證書可以來自內部證書工具、證書頒發機構(CA)或自簽名證書。

問題

對於ESA和SMA，某些SAML SP部署中需要自簽名證書。本文說明如何建立憑證和私密金鑰，以及選擇性地使用密碼短語加密私密金鑰。

解析

- 在Windows上，安裝OpenSSL for Windows。線上提供教程，說明如何完成此操作。
- 在Unix、macOS和Linux上，OpenSSL通常在預設情況下可用。
- 當ESA已經管理證書並且必須匯出證書以供SAML SP使用時，請使用ESA Web UI方法。
- 當必須直接從命令列建立證書和金鑰對時，請使用OpenSSL命令方法。

方法1:在ESA Web UI中建立和匯出自簽名證書

當ESA已經管理證書並且必須匯出證書以供SAML SP使用時，請使用此方法。

建立憑證。

1.在ESA Web UI中，導航至Network > Certificates。選擇Add Certificate，然後選擇Create Self-Signed Certificate。

2.輸入模板欄位:公用名稱、組織、組織單位、城市、州/省、國家以及Duration(118250至12天)。

3.將私鑰大小設定為2048。

Add Certificate	
Add Certificate:	Create Self-Signed Certificate
Common Name:	SAML_SSO
Organization:	Cisco
Organizational Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Duration before expiration:	18250 days
Private Key Size:	2048 1024

完成自簽名證書模板

4.提交證書，稽核結果，然後選擇提交更改。

Certificate Name:	SAML_SSO
Common Name:	SAML_SSO
Organization:	Cisco
Organization Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Signature Issued By:	Common Name (CN): SAML_SSO Organization (O): Cisco Organizational Unit (OU): ESA_TAC Issued On: Sep 20 15:50:27 2019 GMT Expires On: Sep 7 15:50:27 2069 GMT

組態後檢視

匯出證書。

1.在ESA Web UI中，導航至網路>證書>匯出證書。

2.選擇要匯出的證書，建立口令，選擇匯出，然後將檔案儲存到目錄。

附註：用於管理的SAML SSO可以匯入PKCS#12(PFX)證書。如果不需要私鑰加密，則其餘轉換步驟是可選的。

轉換證書。

匯出的證書採用PKCS#12/PFX格式，需要轉換為隱私增強型郵件(PEM)。

運行此OpenSSL命令將PFX檔案轉換為PEM格式。

<#root>

openssl

pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes

<#root>

openssl

pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes

編輯內容並將輸出拆分為兩個檔案。

1.新轉換的檔案需要進行次要編輯。

2.在文本編輯器中開啟兩個空白檔案，並將它們命名為<name>.crt和<name>.key。

3.從轉換的檔案-----復BEGIN CERTIFICATE-----至-----END CERTIFICATE-----一節。

4.將內容貼上到<name>.crt檔案中，然後儲存。

5.從轉換的檔案複製-----BEGIN PRIVATE KEY-----至-----END PRIVATE KEY-----部分。

6.將內容貼上到<name>.key檔案中，然後儲存。

7.現在可以將證書和金鑰載入到配置的SAML SP部分。

方法2:使用OpenSSL命令建立自簽名的憑證和金鑰對

當必須直接從命令列建立證書和金鑰對時，請使用此方法。

建立憑證和金鑰對。

在Unix、Linux或macOS命令列介面中運行OpenSSL命令。用所需的名稱替換域。

<#root>

openssl

```
 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt
```

建立期間，將顯示列出的欄位的提示。

在命令運行的目錄中生成兩個檔案：saml_ssl.crt和saml_ssl.key。

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

加密私鑰(可選；配置不需要)。

附註：請勿重複使用範例密碼短語。此金鑰僅用於示例目的。

此OpenSSL命令採用未加密的私密金鑰(unencrypted.key)並輸出加密的金鑰(encrypted.key):

<#root>

openssl

rsa -des3 -in unencrypted.key -out encrypted.key

<#root>

openssl

rsa -des3 -in saml_sso.key -out saml_secure.key

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

證書和金鑰已準備好用於SAML SSO SP或垃圾郵件SSO SP設定。

相關資訊

Cisco Email Security Appliance - 一般使用者指南

思科內容安全管理裝置 — 最終使用手冊

Cisco Web Security — 最終使用手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。